ROUTING AND RECORD SHEET

SUBJECT: (Optional) Information Security Oversight Office Initiatives Presented to the National Security Council

STAT
STAT

FROM:
Director of Information Services
1206 Ames Building

EXTENSION

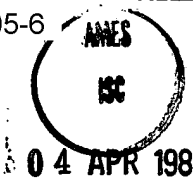
NO. OIS*125*86

10-10

DATE 4 APR 1986

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. EO/DDA 7D18 Headquarters	[illegible] 1986			AMES ISC LOGGED 04 APR 1986
2.				
3. ADDA	9 APR 1986			
4.				
5. DDA	10 [illegible]			
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

FORM 1-79 610 USE PREVIOUS EDITIONS



LOGGED

OIS*125*86
4 APR 1986

MEMORANDUM FOR: Deputy Director for Administration

STAT FROM: [redacted]
Director of Information Services

SUBJECT: Information Security Oversight Office Initiatives presented to the National Security Council

REFERENCE: Attached Office of Security memorandum for DDA signature to the DCI

1. This memorandum provides additional information for your consideration regarding four of the information security initiatives forwarded to the National Security Council (NSC) on 14 November 1985 by the Director, Information Security Oversight Office (ISOO).

2. Background: The Director of ISOO chaired an interagency committee to study ways of improving the Government-wide information security system. This Agency, as well as the rest of the Intelligence Community, was represented on the committee. Each agency studied a particular aspect of the information security system and proposed measures they believed would improve the system. ISOO reviewed all of the proposals, discarded some, re-scoped others and finally selected thirteen to go forward to the National Security Council as ISOO initiatives. When forwarding the initiatives to the NSC, D/ISOO neglected to point out the disagreement among the participating agencies concerning the merit of some of these initiatives. Although the D/ISOO is aware of the Agency opposition to a number of these initiatives, he did not see fit to make it a part of his official correspondence to the NSC. These initiatives have also gained additional support from the Senate Select Committee on Intelligence (SSCI) and the Stillwell Working Group. The Agency specifically opposed the following four initiatives:

Initiative No. 1 - That ISOO issue a directive on security education that includes the establishment of minimum requirements for mandatory training of classifiers of original and derivative classification decisions and the use of classification guides.

Initiative No. 2 - That ISOO issue a directive on agency self-inspections that establishes minimum criteria for internal oversight, including a requirement that each agency routinely sample its classified product.

Initiative No. 3 - That the President amend E.O. 12356 and ISOO amend Directive No. 1 to (i) require employees to report instances of improper classification and (ii) require that agencies provide an effective means for employees to challenge classification decisions free from the fear of retaliation.

Initiative No. 13 - That the President call upon the Attorney General to revise existing guidelines on investigations of unauthorized disclosures.

3. In the attached referent memorandum, the Office of Security (OS) cautions against an erosion of DCI special authorities only in Initiatives 1 and 13. I believe the same potential for erosion exists in ISOO Initiative No. 2. Although internal oversight to ensure against unnecessary or improper classification (Initiative No. 2) would be less difficult for the Agency to deal with than mandatory training of our classifiers (Initiative No. 1), it is, nonetheless, an encroachment on the DCI's special authorities. This initiative, if adopted, would permit ISOO to set internal Agency standards and procedures for inspections. If you choose to recommend DCI action to preserve his special authorities on these issues, I suggest that ISOO Initiative No. 2 be included with Initiatives Nos. 1 and 13.

4. Further, I recommend that this Agency continue to oppose ISOO's Initiative No. 3 in its entirety. There are two issues involved in Initiative No. 3: one, the "requirement" that all federal employees challenge classification decisions they believe to be improper; and two, that agencies provide an "effective means" for employees to challenge classification decisions free from the "fear of retaliation." OS recommends continued opposition to the "requirement" to challenge classification decisions but accepts the statement that there is a need to provide "effective means" for employees to challenge classification decisions. I disagree. This Agency already has an effective means for employees to challenge or question classification decisions. An employee wishing to question or challenge the classification or classification level of a document, can contact the the Agency Security Classification Officer (ASCO) and discuss these concerns. Although classification challenges in this Agency are rare, classification questions are fairly frequent and are routinely referred to the ASCO. If the ASCO is unable to resolve the question or problem, an employee has recourse to the Director, ISOO. Pursuant to E.O. 12356, Sec 5.2, (b)(6) the Director, ISOO shall consider and take action on complaints and suggestions with respect to the administration of the information security program. This

procedure has been used successfully in the past by individuals questioning the classification of documents. Other than using the phrase "fear of retaliation," as part of the initiative, ISOO has not offered, nor am I aware of, evidence of any retaliation against government employees or other individuals who have questioned classification decisions. Finally, we do not oppose the right of an employee to challenge or question a classification decision. Our opposition is based instead on concern over the administrative burden that would be placed on the Agency with no additional advantage to the Agency or the individual.

5. Although we have discussed our concerns with both the Office of Security and the Office of General Counsel, we have been unable to persuade either to our point of view. Nevertheless, I feel obliged to bring these issues to your attention. If you agree with our comments, we are prepared to revise the OS memorandum to the DCI to incorporate OIS concerns.

STAT

Attachment

OIS*125*86
4 APR 1986

MEMORANDUM FOR: Deputy Director for Administration

STAT FROM: [redacted]
Director of Information Services

SUBJECT: Information Security Oversight Office Initiatives presented to the National Security Council

REFERENCE: Attached Office of Security memorandum for DDA signature to the DCI

1. This memorandum provides additional information for your consideration regarding four of the information security initiatives forwarded to the National Security Council (NSC) on 14 November 1985 by the Director, Information Security Oversight Office (ISOO).

2. Background: The Director of ISOO chaired an interagency committee to study ways of improving the Government-wide information security system. This Agency, as well as the rest of the Intelligence Community, was represented on the committee. Each agency studied a particular aspect of the information security system and proposed measures they believed would improve the system. ISOO reviewed all of the proposals, discarded some, re-scoped others and finally selected thirteen to go forward to the National Security Council as ISOO initiatives. When forwarding the initiatives to the NSC, D/ISOO neglected to point out the disagreement among the participating agencies concerning the merit of some of these initiatives. Although the D/ISOO is aware of the Agency opposition to a number of these initiatives, he did not see fit to make it a part of his official correspondence to the NSC. These initiatives have also gained additional support from the Senate Select Committee on Intelligence (SSCI) and the Stillwell Working Group. The Agency specifically opposed the following four initiatives:

Initiative No. 1 - That ISOO issue a directive on security education that includes the establishment of minimum requirements for mandatory training of classifiers of original and derivative classification decisions and the use of classification guides.

Initiative No. 2 - That ISOO issue a directive on agency self-inspections that establishes minimum criteria for internal oversight, including a requirement that each agency routinely sample its classified product.

Initiative No. 3 - That the President amend E.O. 12356 and ISOO amend Directive No. 1 to (i) require employees to report instances of improper classification and (ii) require that agencies provide an effective means for employees to challenge classification decisions free from the fear of retaliation.

Initiative No. 13 - That the President call upon the Attorney General to revise existing guidelines on investigations of unauthorized disclosures.

3. In the attached referent memorandum, the Office of Security (OS) cautions against an erosion of DCI special authorities only in Initiatives 1 and 13. I believe the same potential for erosion exists in ISOO Initiative No. 2. Although internal oversight to ensure against unnecessary or improper classification (Initiative No. 2) would be less difficult for the Agency to deal with than mandatory training of our classifiers (Initiative No. 1), it is, nonetheless, an encroachment on the DCI's special authorities. This initiative, if adopted, would permit ISOO to set internal Agency standards and procedures for inspections. If you choose to recommend DCI action to preserve his special authorities on these issues, I suggest that ISOO Initiative No. 2 be included with Initiatives Nos. 1 and 13.

4. Further, I recommend that this Agency continue to oppose ISOO's Initiative No. 3 in its entirety. There are two issues involved in Initiative No. 3: one, the "requirement" that all federal employees challenge classification decisions they believe to be improper; and two, that agencies provide an "effective means" for employees to challenge classification decisions free from the "fear of retaliation." OS recommends continued opposition to the "requirement" to challenge classification decisions but accepts the statement that there is a need to provide "effective means" for employees to challenge classification decisions. I disagree. This Agency already has an effective means for employees to challenge or question classification decisions. An employee wishing to question or challenge the classification or classification level of a document, can contact the the Agency Security Classification Officer (ASCO) and discuss these concerns. Although classification challenges in this Agency are rare, classification questions are fairly frequent and are routinely referred to the ASCO. If the ASCO is unable to resolve the question or problem, an employee has recourse to the Director, ISOO. Pursuant to E.O. 12356, Sec 5.2, (b)(6) the Director, ISOO shall consider and take action on complaints and suggestions with respect to the administration of the information security program. This

procedure has been used successfully in the past by individuals questioning the classification of documents. Other than using the phrase "fear of retaliation," as part of the initiative, ISOO has not offered, nor am I aware of, evidence of any retaliation against government employees or other individuals who have questioned classification decisions. Finally, we do not oppose the right of an employee to challenge or question a classification decision. Our opposition is based instead on concern over the administrative burden that would be placed on the Agency with no additional advantage to the Agency or the individual.

5. Although we have discussed our concerns with both the Office of Security and the Office of General Counsel, we have been unable to persuade either to our point of view. Nevertheless, I feel obliged to bring these issues to your attention. If you agree with our comments, we are prepared to revise the OS memorandum to the DCI to incorporate OIS concerns.

STAT

Attachment

STAT DDA/OIS/IRMD/IMB, [redacted] dbm (31 March 86)

Distribution:
Original & 1 - Addressee w/atts
1 - DDA Subject
1 - D/Security
1 - C/Policy Branch/OS
1 - OIS subject
1 - OIS chrono
1 - IRMD chrono
1 - IMB/IRMD Subject BLIA-2
1 - IMB/IRMD Chrono
1 - EME/IMB